



M E M O R A N D U M

To: Victoria L. Bradshaw, Secretary
Labor and Workforce Development Agency

Date: May 20, 2008

File No.: 78:155:lb

Project No.: 607.000

From: Employment Development Department

Subject: EVALUATION OF INTERNAL ACCOUNTING AND ADMINISTRATIVE CONTROL
SYSTEM

In accordance with the Financial Integrity and State Manager's Accountability Act of 1983, Government Code, Sections 13400 through 13407, I am submitting the attached report describing the review of our system of internal control for the biennial period ending June 30, 2007.

As statutorily required, the Employment Development Department (EDD) is in compliance with Government Code, Section 12439. Our compliance includes working with the Department of Finance to eliminate unneeded vacant positions from the EDD budget. In addition, the EDD has established new guidelines for managing vacant positions consistent with Assembly Bill 3000 (Chapter 1124, Statutes of 2002) that amended Government Code, Section 12439.

If you have any questions regarding this report, please call Gregory Riggs, Acting Deputy Director, Program Review Branch at (916) 654-7014.

/s/
PATRICK W. HENNING
Director

Attachment

STATE ADMINISTRATIVE MANUAL 20060

**EVALUATION OF INTERNAL ACCOUNTING AND
ADMINISTRATIVE CONTROL SYSTEM**

**AUDIT REPORT
FISCAL YEARS 2005-2007**

May 2008



Arnold Schwarzenegger
Governor
STATE OF CALIFORNIA

Victoria L. Bradshaw
Secretary
LABOR AND WORKFORCE DEVELOPMENT AGENCY

Patrick W. Henning
Director
EMPLOYMENT DEVELOPMENT DEPARTMENT

M E M O R A N D U M

To: Victoria L. Bradshaw, Secretary
Labor and Workforce Development Agency

Date: May 20, 2008

File No.: 78:155:lb
Project No.: 607.000

From: Patrick W. Henning
Employment Development Department

Subject: CERTIFICATION OF INTERNAL ACCOUNTING AND ADMINISTRATIVE CONTROL SYSTEM

As the Director of the Employment Development Department (EDD) effective November 2004, in accordance with the Financial Integrity and State Manager's Accountability (FISMA) Act of 1983, Government Code, Sections 13400 through 13407, I agree that I am responsible for the establishment and maintenance of a system or systems of internal accounting and administrative control within my agency. This responsibility includes documenting the system, communicating system requirements to employees, and assuring that the system is functioning as prescribed and is modified, as appropriate, for changes in conditions; therefore, I certify that our system of internal accounting and administrative control includes:

- A plan of organization that provides segregation of duties appropriate for proper safeguarding of State assets.
- A plan that limits the access of State assets to authorized personnel who require these assets in the performance of their assigned duties.
- A system of authorization and recordkeeping procedures adequate to provide effective accounting control over assets, liabilities, revenues, and expenditures.
- An established system of practices to be followed in the performance of duties and functions in each of the State entities.
- Personnel of a quality commensurate with their responsibilities.
- An effective system of internal review.
- Guidelines for managing vacant positions consistent with Assembly Bill 3000 (Chapter 1124, Statutes of 2002) that amended Government Code, Section 12439. In addition, the EDD works harmoniously with the Department of Finance to eliminate unneeded vacant positions from the Departmental budget.

Victoria L. Bradshaw, Secretary
May 20, 2008
Page two

The EDD's Audit and Evaluation Division (A&ED) has audited our internal control structure within the biennial period ending June 30, 2007, under the requirements of Government Code, Section 13402, et seq., in accordance with the *Government Auditing Standards*, published by the Government Accountability Office; *International Standards for the Professional Practice of Internal Auditing*, published by the Institute of Internal Auditors; Department of Finance's 2006 edition of the *Audit Guide for the Evaluation of Internal Control*; State Administrative Manual (SAM), Sections 4800 through 5180, State Information Management Principles; and the National Institute of Standards and Technology Guidelines.

The audit included tests considered necessary in determining that accounting and administrative controls are in place and operative. The A&ED coordinated a mandated enterprisewide self-certification process that required the management team to complete an internal control checklist and certify that a satisfactory system of internal control is in place and functioning as intended. To verify the reliability of the self-certification process, the A&ED conducted a limited scope review.

The audit and review of the enterprisewide self-certification did not reveal any significant internal control weakness that would be considered pervasive in their effects on the accounting and administrative controls. The A&ED identified other reportable weaknesses that need correction by management to maintain EDD's compliance with the FISMA Act of 1983. The findings, with appropriate corrective actions taken to address the recommendations, are presented in the Findings and Recommendations section of the attached SAM 20060 Evaluation of Internal Accounting and Administrative Control System Audit Report for Fiscal Years 2005-2007, dated May 2008.

/s/
PATRICK W. HENNING
Director

Attachment

cc: Governor Arnold Schwarzenegger
Members of the Legislature
Elaine Howle, State Auditor
Michael C. Genest, Director, Department of Finance
Susan Hildreth, State Library

M E M O R A N D U M

To: Patrick W. Henning, MIC 83

Date: May 20, 2008

File No.: 78:155:lb

From: Tonia Lediju
Employment Development Department

Subject: STATE ADMINISTRATIVE MANUAL 20060 EVALUATION OF INTERNAL
ACCOUNTING AND ADMINISTRATIVE CONTROL SYSTEM AUDIT REPORT FOR
FISCAL YEARS 2005-2007

The Audit and Evaluation Division (A&ED) completed its audit of the Employment Development Department (EDD) internal control structure in effect as of June 30, 2007. The audit was conducted in accordance with the *Government Auditing Standards*, published by the Government Accountability Office; the *International Standards for the Professional Practice of Internal Auditing*, published by the Institute of Internal Auditors; Department of Finance's 2006 edition of *Audit Guide for the Evaluation of Internal Control*; State Administrative Manual (SAM), Sections 4800 through 5180, State Information Management Principles; and the National Institute of Standards and Technology Guidelines. The audit included tests considered necessary in determining that accounting and administrative controls are in place and operative.

The EDD's management is responsible for establishing and maintaining adequate internal controls. This responsibility, in accordance with Government Code, Section 13402, et seq., includes documenting internal control, communicating requirements to employees, and assuring that internal control is functioning as prescribed. In fulfilling this responsibility, estimates and judgments by management are required to assess the expected benefits and related costs of control procedures.

The objectives of internal accounting and administrative control are to provide management with reasonable, but not absolute, assurance that:

- Assets are safeguarded against loss from unauthorized use or disposition.
- Transactions are executed in accordance with management's authorization and recorded properly to permit the preparation of financial statements in accordance with generally accepted accounting principles.
- Financial operations are conducted in accordance with policies and procedures established in the SAM.

The audit did not reveal any significant internal control weakness that would be considered pervasive in their effects on the accounting and administrative controls. The A&ED did identify other reportable weaknesses that need to be addressed by management to maintain EDD's compliance with the FISMA Act of 1983. The findings, with appropriate recommendations and responses, are presented in the Findings and Recommendations Section of this report.

In A&ED's opinion, EDD's accounting and administrative control as of June 30, 2007, taken as a whole, was sufficient to meet the above objectives.

Because of inherent limitations in any internal control structure, errors or irregularities may occur and not be detected. Specific limitations that may hinder the effectiveness of an otherwise adequate system of controls include, but are not limited to: resource constraints, poor business decisions, circumvention of policies and procedures, misstatements due to unintentional errors, and fraud.

/s/

TONIA LEDIJU, Chief
Audit and Evaluation Division

Project Lead: Ed Murray, Manager

Audit Team: Roger Remedios, Manager
Elaine Dement, Supervisor
Cathy Dockter, Supervisor
Will Fong, Supervisor
Vallery Walker, Supervisor
Annabel Alvarez
Velma Bardin
Luisa Doi
Karen Gee
Donna Gracia
James Graston
Roman Hernandez
Edmond Kwan
Tehani Matthews
Rau Palagummi
Ron Perez
Carrie Rosell
Andrea Segal
Derrick Yee

**STATE ADMINISTRATIVE MANUAL 20060
EVALUATION OF INTERNAL ACCOUNTING AND
ADMINISTRATIVE CONTROL SYSTEM**

AUDIT REPORT FOR FISCAL YEARS 2005-2007

TABLE OF CONTENTS

	Page
Executive Summary	1
Background	2
Objective.....	4
Scope	4
Methodology.....	4
Summary	5
Conclusion	5
Findings and Recommendations.....	A-1
Information Technology Finding No. 1 and Auditee's Response	A-1
Information Technology Finding No. 2 and Auditee's Response	A-2
Information Technology Finding No. 3 and Auditee's Response	A-3

Employment Development Department

Audit and Evaluation Division

Executive Summary

The Financial Integrity and State Manager's Accountability (FISMA) Act of 1983, as stated in Government Code (GC), Sections 13400 through 13407, requires the heads of State agencies to establish and maintain a system of internal control and, on a biennial basis, conduct an internal review, and prepare a report on the adequacy of system(s) of internal control.

The California Employment Development Department (EDD) Director accepts full fiduciary responsibility. As mandated, this responsibility includes documenting the system; communicating system requirements to employees; and assuring that the system is functioning as prescribed and is modified, as appropriate, for changes in conditions.

In 2006, the Department of Finance (DOF) modified the FISMA reporting requirements, thus allowing departments who had begun reviews prior to this time, to continue under the traditional State Administrative Manual (SAM) requirements as outlined in DOF's 2006 edition of the *Guidance for the Evaluation of Internal Control*.

The EDD has completed the required agency biennial internal accounting and administrative control audit in accordance with the traditional SAM scope and methodology. This audit did not identify any significant internal control weakness that would be considered pervasive in their effects on the accounting and administrative controls. However, the audit did identify other reportable weaknesses that are actively being addressed by management to ensure that the EDD remains in compliance with the FISMA Act of 1983.

To align with DOF's current SAM guidelines, the EDD proactively established three major enterprise solutions for managing and protecting assets:

- 1) The Information Technology Governance Council (ITGC) ensures that the information technology (IT) development, deployment, and maintenance of electronic services meets the needs of the citizens of California by using a collaborative risk-based approach for decision-making.
- 2) The EDD Strategic Business Plan addresses the need for the enterprise to respond to identified changes and coordinate goals through statewide programs.
- 3) The Enterprise Risk Management (ERM) program further enables EDD's leadership to identify, quantify, and mitigate risks as the EDD undertakes its mission.

Employment Development Department

Audit and Evaluation Division

The compilations of these solutions in their entirety or in part are methods that assist the EDD Director and other EDD leaders in adequately ensuring that processes have been implemented to safeguard assets; provide effective accounting control, accuracy, and reliability; promote operational efficiency; and encourage adherence to adopted departmental policies and procedures.

Background

Effective July 12, 2006, Chapter 69, Statutes 2006 amended the FISMA Act of 1983, which requires the heads of State agencies to conduct an internal review, and prepare a report on the adequacy of system(s) of internal control on a biennial basis. The amendment specifies that a certification letter alone is no longer sufficient to meet the statutory requirement. This review must be done in accordance with the new guidelines prepared by the DOF. These guidelines require departments to:

- Submit a certification letter, audit reports, and a Corrective Action Plan (CAP) and schedule for the identified inadequacies and weaknesses. The CAP and schedule must be updated every six months until resolved.
- Conduct all internal control audits using a risk-based approach.
- Comply with the Standards for the Professional Practice of Internal Auditing, Government Auditing Standards, and Generally Accepted Auditing Standards.
- Perform risk assessments based on the management frameworks designed by the Commission of Sponsoring Organizations (COSO) and the National Institute of Standards and Technology (NIST).

The DOF permitted departments who started the SAM cycle prior to announcing the new SAM guidelines in 2007 to continue with the traditional audit approach, which includes the following transaction cycles: Information Access/Data Integrity Controls, Budget, Cash Receipts, Receivable, Purchasing, Cash Disbursements, Revolving Fund, Personnel and Payroll, Contracts, Fixed Assets, and Financial Reporting.

In 2005, the EDD established an enterprise ITGC that ensures the IT development, deployment, and maintenance of electronic services meets the needs of the citizens of California. The ITGC consists of the Chief Deputy Director and other Executive Staff. The ITGC is responsible to ensure the highest level of governance; it uses a collaborative risk/value approach to decide IT policies, allocate resources, and manage and mitigate IT risks.

Employment Development Department

Audit and Evaluation Division

In May 2007, the Director released EDD's Strategic Business Plan (the Plan) for the period 2007 through 2011. The Plan addresses the need for the enterprise to respond to changes within its business environment and to measure and modify EDD's direction in response to these changes. The Director also recognizes the need to overcome internal and external operating constraints such as an aging and knowledgeable workforce on the verge of retirement; outdated, redundant, and cumbersome technology; and significant decreases in federal funding that supports EDD programs.

In September 2007, EDD's Director charged the Audit and Evaluation Division (A&ED) and EDD's Information Security Office (ISO) to develop and launch an Enterprise Risk Management (ERM) program to align with DOF's SAM guidelines as well as other federal governing stakeholders.

The focus of the ERM program is to enable EDD's leadership to further identify, quantify, and mitigate risks involved in accomplishing its mission. The ERM framework prescribes best practices for evaluating the enterprise's programmatic risk as well as IT system risk, and ensures effective reporting, compliance with applicable laws, regulations, and EDD policies.

The ERM council is comprised of the Chief Deputy Director and other Executive Staff who are responsible to ensure that the basis for determining how the risks should be managed is adequate to minimize the impact on the achievement of EDD's goals and objectives.

In an effort to proactively minimize risk and maintain a high standard of customer service, long before the newly formed EDD ERM program and the reformed DOF SAM requirements, the EDD Director recognized that it is more prudent and beneficial to the enterprise to:

- Prioritize these goals and objectives outside of the programmatic parameters.
- Collaboratively identify significant IT infrastructure risks.
- Deploy needed EDD technology through a collaborative governance process.

The ITGC and the ERM council will work in partnership to adequately ensure that enterprise risks are identified, quantified, mitigated, and that accepted risks have a minimal impact on the overall mission of the organization.

Employment Development Department

Audit and Evaluation Division

Objective

The objective of this audit is to determine if the EDD has established and maintained internal accounting and administrative control systems that provide management with reasonable, but not absolute, assurance that:

- Assets are safeguarded against loss from unauthorized use or disposition.
- Transactions are executed in accordance with management's authorization and are recorded properly to permit the preparation of reliable financial statements.
- Financial and business operations are conducted efficiently and effectively in accordance with the SAM and EDD policies and procedures.

Scope

This audit was limited to the testing and evaluation of internal controls and control procedures for the period of July 1, 2005 through June 30, 2007, and included the review of existing policies and procedures, as well as the examination and test of recorded transactions to determine compliance with established control procedures and good business practices. Audit fieldwork, which included both field and headquarters offices, was conducted on an ongoing basis during the period June 26, 2006 through October 18, 2007.

Methodology

The A&ED evaluated EDD's internal control structure for Information Technology, Trust Fund, and 4 of the 11 traditional SAM cycles: (1) Cash Receipts, (2) Cash Disbursements, (3) Personnel and Payroll, and (4) Contracts.

The A&ED evaluated the compliance of EDD's IT infrastructure to the fundamental principles, and policies and procedures mandated by the DOF for governing IT, as described in the SAM, Sections 4800 through 5180, State Information Management Principles; and the NIST standards.

To determine the overall adequacy of EDD's control practices and procedures, the A&ED performed surveys when applicable, conducted interviews, observed operations, tested and recorded transactions, and performed other audit procedures as deemed necessary.

To meet SAM requirements for the Contracts cycle, the A&ED relied on its internal audit work and the Department of General Services' (DGS) peer review, which was conducted to satisfy the requirements for being granted as a recipient of DGS's contract delegation authority for the period November 1, 2004 through October 31, 2006.

Employment Development Department

Audit and Evaluation Division

To further ensure management's compliance with GC, Section 13402, et seq., the A&ED coordinated a mandated enterprisewide self-certification process that required the EDD leadership team complete an internal control checklist and certify that a satisfactory system of internal control is in place and functioning as intended. To verify the reliability of the self-certification process, the A&ED conducted a limited scope review.

The sample testing conducted in this audit was scientifically selected by EDD's statistician and statistically represents the complete data set. The results of the sample testing can be projected to the total populations.

Summary

This audit did not identify any significant internal control weaknesses that would be considered pervasive in their effects on the accounting and administrative controls. However, the audit did identify EDD's need to improve safeguarding of assets and to establish appropriate control procedures to ensure the integrity and security of IT assets.

The A&ED identified:

- The EDD has not consistently installed patches and/or security upgrades on EDD's desktops and laptops.
- The EDD's current Intrusion Detection and Prevention System does not provide the expected level of protection to adequately ensure the integrity and security of information assets.
- The EDD has not developed and distributed formal, written IT infrastructure policies.

The matrix presented as Appendix A provides a summary of each finding and appropriate recommendations.

Conclusion

The EDD Director and the EDD leadership team remains committed to ensuring that the EDD remains in alignment with the FISMA Act of 1983 and the DOF SAM guidelines. Further, the Director believes that the establishment of EDD's three major enterprise solutions for managing and protecting assets will continue to assist the leadership in adequately fulfilling the requirements of the FISMA Act of 1983 as outlined in GC, Sections 13400 through 13407.

Employment Development Department

Audit and Evaluation Division

The EDD has met the requirements of Senate Bill 1452 by establishing a framework in which the A&ED is free to conduct their work independently. To ensure audit independence, the A&ED reports administratively to the Chief Deputy Director.

The A&ED conducted this review under the requirements of GC, Section 13402, et seq., and in accordance with the *Government Auditing Standards*, published by the Government Accountability Office; and the *International Standards for the Professional Practice of Internal Auditing*, published by the Institute of Internal Auditors. The A&ED limited its review to those areas specified in the Methodology section of this report.

/s/

TONIA LEDIJU, Chief
Audit and Evaluation Division

Date: May 14, 2008

Staff: Ed Murray, Audit Manager
Roger Remedios, Audit Manager
Elaine Dement, Audit Supervisor
Cathy Dockter, Audit Supervisor
Will Fong, Audit Supervisor
Vallery Walker, Audit Supervisor
Annabel Alvarez, Auditor
Luisa Doi, Auditor
Karen Gee, Auditor
Donna Gracia, Auditor
James Graston, Auditor
Roman Hernandez, Auditor
Edmond Kwan, Auditor
Tehani Matthews, Auditor
Rau Palagummi, Auditor
Ron Perez, Auditor
Carrie Rosell, Auditor
Andrea Segal, Auditor
Derrick Yee, Auditor

STATE ADMINISTRATIVE MANUAL 20060 FINDINGS AND RECOMMENDATIONS

Fiscal Years 2005-2007

Transaction Cycle	Finding No.	Reportable Finding	Summary of Finding	Criteria	Recommendation	Auditee's Response	Auditor's Comment
Information Technology (IT) Controls	1	The Employment Development Department (EDD) has not consistently installed patches and/or security upgrades on EDD's desktops and laptops.	<p>Patches and/or security upgrades were not always current because the tools currently used by the EDD did not always capture, push out, or detect missing patches and/or security upgrades correctly.</p> <p>In addition, laptops were not always connected to the network regularly or for a sufficient length of time to receive the required patches and/or security upgrades.</p>	<p>The State Administrative Manual (SAM), Section 4841.2, Information Integrity and Security states in part, "Each agency must provide for the integrity and security of its information assets."</p> <p>The EDD Information Security Policy, Section 7.2.4.2, Equipment Logical Maintenance states in part, "Managers must ensure regular logical maintenance of all local information processing equipment in accordance with IT Branch."</p> <p>The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-40 Version 2, Creating a Patch and Vulnerability Management Program.</p>	<p>The Audit and Evaluation Division (A&ED) recommends:</p> <p>The IT Branch analyze the current software tool to determine if it adequately meets the Enterprise requirements to manage the deployment and detection of missing patches and security upgrades.</p> <p>The IT Branch and the Information Security Office (ISO) collaboratively manage security patches and security upgrades and develop the applicable policy.</p>	The EDD agrees to the recommendations.	<p>The A&ED concurs with the response.</p> <p>The A&ED will follow-up on a quarterly basis.</p>

STATE ADMINISTRATIVE MANUAL 20060 FINDINGS AND RECOMMENDATIONS

Fiscal Years 2005-2007

Transaction Cycle	Finding No.	Reportable Finding	Summary of Finding	Criteria	Recommendation	Auditee's Response	Auditor's Comment
Information Technology (IT) Controls	2	The Employment Development Department's (EDD) current Intrusion Detection and Prevention System (IDPS) does not provide the expected level of protection to adequately ensure the integrity and security of information assets.	The Audit and Evaluation Division (A&ED) interviewed IT Branch management who stated that the IDPS does not work on a continuous basis as intended. As a result, the EDD contracted with a private vendor who has the expertise to conduct an "ethical hack" penetration test. The results of this test will aid the EDD with process improvement.	The State Administrative Manual (SAM), Section 4841 states, "Each agency must provide for the proper use and protection of its information assets." The National Institute of Standards and Technology (NIST) SP 800-31, Intrusion Detection Systems, recommends that organizations implement an automated Intrusion Detection System to monitor the events occurring in a computer system or network, and analyze them for signs of security breaches.	The A&ED recommends: The IT Branch management review the results of the "ethical hack" penetration test and establish and implement an adequate intrusion detection and prevention policy to maintain the integrity and security of EDD's information assets.	The EDD agrees to the recommendations.	The A&ED concurs with the response. The A&ED will follow-up on a quarterly basis.

STATE ADMINISTRATIVE MANUAL 20060 FINDINGS AND RECOMMENDATIONS

Fiscal Years 2005-2007

Transaction Cycle	Finding No.	Reportable Finding	Summary of Finding	Criteria	Recommendation	Auditee's Response	Auditor's Comment
Information Technology (IT) Controls	3	The Employment Development Department's (EDD) has not developed and distributed formal, written IT infrastructure policies. The EDD has adopted best practices based on industry standards as an interim measure to the development of formal policies and procedures to provide for the integrity and security of its information assets.	<p>The Audit and Evaluation Division (A&ED) identified that the following formal written policies have not been developed:</p> <ul style="list-style-type: none"> • Technology Upgrade Policy • Security Patches and Security Upgrade Policy • Firewall Configuration Policy • Server Configuration Policy • Server Hardening Policy 	<p>The State Administrative Manual (SAM), Section 4841.2 states in part, "Each agency must provide for the integrity and security of its information assets by: . . . 3. Establishing appropriate departmental policies and procedures to protect and secure IT infrastructure."</p> <p>The SAM, Section 4841.1 states in part, "The Information Security Officer is required to oversee agency compliance with policies and procedures regarding the security of its information assets."</p> <p>The SAM, Section 4841.1 states in part, "Agency information technology management is responsible for... integrity of the agency's information assets and managing the risks...information."</p> <p>The SAM, Section 4841.6 states in part, "The responsibilities of. . ."</p>	The A&ED recommends that Executive Management continue to provide guidance to the Information Security Office and the IT Branch on their roles and responsibilities to develop and distribute IT infrastructure policies to provide for the integrity and security of its information assets.	" . . . EDD management recognizes the value of policy to clearly set forth standards, expectations, and responsibilities for IT security. As such, EDD management plans to develop IT policies in the areas identified . . ."	<p>The A&ED concurs with the response.</p> <p>The A&ED will follow-up on a quarterly basis.</p>

The California State Employment Development Department, as a recipient of federal and state funds, is an equal opportunity employer/program and is in compliance with Section 504 of the Rehabilitation Act and the Americans with Disabilities Act.

Special requests for alternate formats need to be made by calling 916-654-7000.